METHOD OF MANAGING THE DISPLAY OF EVENT SPECIFICATIONS WITH CONDITIONAL ACCESS

This invention concerns a method of managing the display of event specifications with conditional access, in particular in the Pay-TV domain.

5   In the conditional access systems, in particular in the digital Pay-TV domain, a digital data flow is transmitted towards the television set. This flow is encrypted in order to be able to control the use thereof and to define certain conditions for such use. This encryption is made thanks to certain control words, which are changed at regular intervals (typically between 5

10   and 30 seconds) in order to deter any attack aiming to find such a control word.

For the receiver to decipher the encrypted flow with these control words, these are sent to the receiver regardless of the flow in control messages (ECM) encrypted by an exclusive key of the transmission system between

15   a management centre and a user unit security module. In fact, the security operations are carried out in a security module (SC), which is generally made as a smart card, intended to be tamper-proof. This module can be either of the removable type or directly integrated to the receiver.

At the time of the decryption of a control message (ECM), it is verified, in

20   the security module (SC), that the right to access to the flow in question is present. This right can be managed by some authorization messages (EMM), which load such a right into the security module. Other solutions can also be considered, such as sending decryption keys.

In the following description, the term "event" will designate video, audio (for

25   example MP3) or data content (game program for example), which are encrypted according to the known method of control words, each event being able to be ciphered by one or more control words, each of them having a given validity duration.

The accounting of the use of such events is today based on the principles of subscription, events purchase or payment by time unit.

The subscription allows the definition of a right associated with one or more broadcasting channels transmitting these events and allows the user to access to these channels in clear if the right exists in his/her security module.

At the same time, it is possible to define certain rights pertaining to a particular event, such as a film or a football match. The user can acquire this right (purchase for example) and this event will be specifically managed by this right. This method is known under the appellation "pay-per-view" (PPV).

A control message (ECM) not only contains the control word, but also the conditions for that word to be sent back to the receiver/decoder. At the time of the decryption of the control words, it will be verified if, in the security module, there is a right associated with access conditions stated in the message.

Whenever the comparison is positive the control word is returned to the user unit. This control word is contained in an ECM control message, which is encrypted by a transmission key.

For the right to be present in the security module, this is generally loaded in this module by an authorization message (EMM) which is, for security reasons, generally encrypted by a different key called right key (RK).

According to a known Pay-TV broadcasting form, the three following elements are necessary for deciphering an event at a given time:
- the data related to the event encrypted by one or by a plurality of control words (CW),
- the ECM control message(s) containing the control words (CW) and the access conditions (AC)

- the corresponding right stored in the security module allowing verification of said access conditions.

The principles described above are also used whenever one wishes to make the list of the channels, services or events visible to a user, channels services or events for which he/she has access as well as for those for which he/she can acquire the rights. For that purpose, an electronic program guide (EPG = Electronic Program Guide) is used and the events or channels for which the rights are already acquired are displayed for example in green, and in red those for which the rights have not been acquired.

When the rights' characterization is simple, for example when the user has subscribed to certain stated services for one determined validity duration, it is easy to generate an EPG that takes these rights into account. On the contrary, when one wishes to manage certain more complex rights, to offer promotions or to use conditions which have not been allowed in the subscription, the current systems do not allow the easy management of these elements.

The International patent application WO 97/42762 describes a data access system that can be particularly used in the Pay-TV domain. In this system, authorization messages are sent to the users' decoders. These messages contain, conventionally, the access rights to Pay-TV events. Furthermore, they contain some pointers, which indicate a location allowing the acquisition of additional data. This additional data can particularly consist in clear data relating to the events themselves or to certain software. This data is connected with the decoder and is generally accessible without any decryption. It is not contained in the authorization messages. This system does not allow the management of the security aspects related to complementary data and does not allow the management of variable

access conditions according to the existing rights for each user, given that on principle these access conditions must be made secure.

This invention intends to compensate for the drawbacks of the prior art devices, by creating a device in which it is possible to manage complex
5 rights thus offering great flexibility of use to a distributor.

This aim is reached by a method of managing the display of event specifications with conditional access, including the following steps:
- sending data forming an electronic program guide (EPG) to a decoder (STB), this electronic guide serving to display the events
10 which will be broadcasted, these data including, for each event, at least one identifier, textual data and a condition block comprising the conditions required for the access to this event,
- sending at least one authorization message (EMM) to a security module (SC) associated with the decoder, this message defining
15 access rights to an event;
characterized in that the method furthermore comprises the following steps:
- sending the condition block (PECM) to said security module (SC),
- processing, in the security module, the access condition contained in said condition block (PECM), and
20 - return by the security module of a message indicating, according to the access condition for each event and to the access rights contained in the security module, if the right exists or not for each event in the security module.

This invention and its advantages will be better understood with reference
25 to the description of a particular embodiment and to the enclosed drawings, in which:
- Figure 1 shows schematically an embodiment of an electronic guide (EPG) according to the prior art;

- Figure 2 shows schematically the contents of a control message (ECM) used in the embodiment of figure 1;
- Figure 3 shows the content of a control message (ECM) according to this invention;
- Figure 4 shows the contents of a condition block used in the system according to the invention; and
- Figure 5 represents an embodiment of an electronic guide EPG according to the invention.

Figures 1 and 2 describe known systems of the prior art. In these systems, the data composing the electronic program guide EPG is transmitted by a service channel and is made up of timetable and textual data, such as, in particular, the event title, the description and maybe some comments. The EPG data also contains the service to which this event is related to as far as access right is concerned, the services being referred to as for example S1 to S48.

At the same time, the broadcasted event is accompanied by the control messages ECM which contain a certain number of preset fields, having references 11 to 14 in Figure 2, such as in particular the identifier event (field 13), the service to which it is related (field 14), the control word CW (field 11), the broadcasting time and date (field 12) and a possible credit associated to the event. Thanks to this structure preset by fields, the message structure is defined in such a way that for example on field 14, the number of a service SID will always be found.

This service is initialized by an authorization message EMM, which has the aim of defining a subscription block in the SC security module, this block containing among other things the validity duration of this service.

To display the electronic guide (EPG) on a user's television set, the decoder STB reads the rights contained in the SC security module, that is to say the aforementioned blocks. More precisely, it determines, according

to these rights, the list of available services as well as the duration or validity date of each service. Thus, the decoder has on the one hand a database originating from the security module and containing the list of the available services with their validity duration and, on the other hand, a

5   database intended for the EPG, which contains the list of events, the service to which it is related to and the diffusion date.

For each event, the decoder can thus verify if the security module has the right for the service in question and if this right will be valid at the moment of the event broadcasting. On the basis of the result of this comparison, the

10   event will be displayed in the EPG, for example in red if the right is not acquired and in green if this right is acquired and thus present in the security module.

In Figure 1, "Yes" is displayed in the last column of the EPG facing the event in question if the right for this event is acquired, and "No" if the right

15   is not acquired.

At the moment of the broadcasting of an event, the ECM control messages, containing the control words CW and associated to this event, are processed in the security module in such a way that the existence of the rights associated to this event are verified. If the rights exist, each ECM

20   control message is processed so that the control words CW that it contains are extracted therefrom. This control word is then sent to the decoder, which deciphers the data that has been encrypted with this specific control word.

This embodiment operates perfectly when the conditions are simple, for

25   example when a user has subscribed to a services package. In this case, the decoder compares the contents of the preset fields in the data composing the EPG with the contents of the security module memory and obtains a reply which can be directly used.

In particular when one wishes to propose promotional offers, it can be necessary to define complex conditions, for which a preset fixed fields structure is not adapted. An example of such a promotional offer consists in allowing a free access to a range of channels, for the birthday of each subscriber. With a conventional system such an offer can be proposed, but at the expense of a large complication. In fact, to allow this, it is necessary to create additional rights, more precisely 365 subscription blocks, each one corresponding to one day of the year. These rights are managed like the other rights, which means that they are transmitted by certain EMM authorization messages. These messages must be sent again and again to all the beneficiaries, in order to be sure that everyone has received the rights.

On receipt of this message, a new subscription block will be created in the security module for this single use. It should be noted that these messages will absorb part of the bandwidth and part of the cryptographic means, particularly because of the high level encryption of these messages.

Another example of a promotional offer consists in invoicing a given event on the basis of several different amounts according to subscription types. The holder of a subscription for sport themed channels can for example pay a football match at a determined price, while people not having this kind of subscription must pay another amount for the same football match. In the present situation, it is not possible to manage this type of rules because the identification of the event is strictly identical for all the users, while the access conditions to this event depend on the event and on the parameters set for a user.

Today, according to the prior art, the solution would consist in sending an EMM authorization message pertaining to each user with the amount for the event having taken into account his/her specific conditions. We can

easily imagine how many messages must be transmitted to satisfy all the users.

More generally, to be able to apply certain particular conditions for a particular event, it is necessary to have these conditions established in advance in the subscription of the users in question. If this is not the case, the management of the particular cases can prove to be difficult or even impossible. In all cases, to generate particular rights on the security module, it is necessary to dispatch certain EMM authorization messages, at such a sufficient frequency to be sure that the majority of the users have received the intended rights.

This embodiment is not very convenient because of the fact that it takes up a large amount of memory and the traffic of the authorization messages EMM does not take full advantage of the available bandwidth.

In figure 3, which describes an embodiment of the invention, the control message ECM does not contain any more a data to a preset location, but an operation Op. This is written under a request form, using for example a syntactic language such as the one known under the acronym SQL (Structured Query Language).

The present invention is particularly advantageous in comparison with the prior art known systems because of the fact that the conditions defined by requests of the SQL type can be imagined, modified or used in a very flexible way, at any time. Being free of preset data fields in the control messages ECM opens the way to combinations not anticipated at the starting point of the system and therefore not set in the users' subscription.

Consequently, with this simplified management, it is possible to propose very diversified offers, even for very small groups. It is thus possible to generate well target offers that are close to the company's marketing views.

At the time of the processing of such an ECM control message, the operation Op is treated by the SQL motor of the security module SC and the return or no-return of the control word CW contained in this same message will depend on the result.

5   As for ECM control messages, it is also considered, within the context of the invention, to replace the fields of an EMM authorization message by a request of type SQL.

The data memorized in the security module, defining the subscription blocks, remains unchanged, only the operations on these data change.

10 As example, a request of this type could be:
- Service S22 valid or birthday date = 10 October.

Another example of complex request for an impulsive purchase could be:
- If the security module contains the rights for S1, S8 and S12 services, then deduce an amount of 4 USD for the Ev 1 event, if not,
15   then deduce an amount of 5 USD for this event.

In this embodiment, the decoder STB is not authorized to process a complex request in SQL language, mainly for security reasons.

In the context of this invention, the solution consists in modifying the data transmitted to the EPG, this modification consisting in including in these
20 data a new block, which is a partial copy of the control message ECM that will be transmitted with the event in question.

This block called condition block (PECM) comprises at least the same SQL request as the control message from which it is derived. According to the chosen implementation, the other fields such as the control word can be
25 removed. Obviously, the control messages ECM are transmitted when the event is visualized by the user, since they contain the control words CW. On the contrary, the conditional blocks must be sent in advance since they

are used to form the EPG which allows the user to visualize in advance the rights he/she has already acquired and those he/she can acquire.

On the receipt of these data by the EPG, this PECM block will be transmitted to the security module, which is able to process complex requests, especially in SQL language.

This PECM block is illustrated in figure 4. The security module will process this condition block in a conventional way and will be able to extract the SQL request therefrom. The conditions defined in this request are analyzed in the security module and the request result is retransmitted to the STB decoder. Thanks to this result, the EPG can be displayed in the way previously explained, with reference to the description of the prior art.

This process is schematically represented by figure 5. More particularly, the data permitting to form the EPG are transmitted to the decoder STB. A condition block PECM, containing, under the form of SQL request, the operation that permits the definition of the access conditions, is formed and then transmitted to the security module SC. This module processes the SQL request. The conditions of the SQL request are compared with the rights inscribed in the security module so that the events for which the rights are acquired or can be acquired can be determined. These available rights are associated with the EPG data. The list of the events is then displayed on the user's television set, distinguishing for each event, whether the security module has the rights or not.